Policy Group	IT Services	**Policy Number**	SUP-ITS-06	جـامـعـة زايـد ZAYED UNIVERSITY
Responsible Office	Office of the CAFO	**Distribution**	External	
Date Approved	4 October 2020	**Effective Date**	4 October 2020	
Date Last Reviewed	30 September 2020	**Due Date for Next Review**	30 September 2023	

POLICY
Password Security

1. Purpose

The purpose of this policy is to establish the rules for the creation, distribution, safeguarding, termination, and reclamation of the Zayed University user authentication mechanism, i.e. user ID and password.

2. Application

This policy applies to Zayed University faculty members, staff members, students, third-party contractors, vendors, and any such entity that is associated with Zayed University information, data, software, resources, and hardware and related processing facilities, and in anyway interacts with the information assets of Zayed University.

3. Policy

3.1 All passwords, including initial passwords, must be constructed and implemented as per ZU IT Department (ITD) information security management rules.

3.2 Users are responsible for all activity performed with their individual user-ID. User-IDs may not be utilized by anyone other than the individuals to whom they have been issued. Users must not allow others to perform any activity with their user-IDs. Similarly, users must not perform any activity with IDs belonging to other users.

3.3 Users should not circumvent password entry with auto logon, application remembering, embedded scripts or hard coded passwords in client software. Exceptions may be made for specific IT applications (e.g. automated backup, laptop re-imaging software) with the approval of the IT Director.

3.4 User accounts that have system-level privileges granted through group memberships, or programs such as "sudo" or “Domain Admins” must have a unique password for each account that is clearly different from the passwords used for all other accounts held by that user.

3.5 All system-level passwords (e.g., root, enable, network administrator, and application administration accounts) must be changed at least once every 15 days, to reduce the risk of compromise.

3.6 All system-level password changes must be pre-approved by the appropriate manager.

3.7 Passwords stored in electronic format, e.g. in a database, spreadsheet or other file, should be encrypted to prevent easy disclosure.

3.8 Passwords must not be divulged to anyone. ZU ITD and IT contractors will not ask for user account passwords.

3.9 If the security of a password is in doubt, the password must be changed immediately.

3.10 ZU network administrators must not circumvent the Password Policy for any reason.

3.11 Computing devices must not be left unattended without enabling a password protected screensaver or logging off the device.

3.12 The passwords for the servers, critical services, and network devices must always be stored in envelopes in a security safe box. Access to the safe box is restricted to appropriate administrative roles within ITD (ITD Director, IT Infrastructure Manager, System Administrator, Network Manager, Network Administrator and Application Manager).

3.13 ITD will require users to change their passwords every 90 days.

3.14 ITD will restrict users from changing their passwords immediately.

3.15 ITD will enforce Password History to discourage users from alternating between several common passwords.

3.16 ITD will enforce user account management controls to lock user accounts after a defined number of failed authentication attempts.

3.17 ITD will provide guidelines or manuals to accomplish this policy.

4. Related Policies and Laws

SUP-ITS-04 Information Security

Telecommunications Regulatory Authority (TRA) Regulations for Information Technology Security in Federal Entities

5. Administration

This policy is administered by the Information Technology Department.

6. Revision History

Date	Revision
4 October 2020	President's Decree issued (PD #90 of 2020).
30 September 2020	Approved by the University Council.
31 May 2020	Non-substantive change: Added External Distribution.
10 October 2019	Reviewed by the VP, CAFO, Legal Advisor and Internal Auditor. Revision: • Clarify the Application section.
7 May 2019	Reviewed by CAFO Management Council and endorsed for further approval. Revisions as per requirement from Telecommunications Regulatory Authority (TRA) Regulations for Information Technology Security in Federal Entities. • Policy section: #2 Added user's responsibility with regards to their User-IDs

	• Policy section: #5 Amended from 45 to 15 number of days for password change • Policy section: # 14 Added changing of passwords • Policy section: #15 Added Password History • Policy section: #16 Added User Account management controls
12 March 2018	Approved by the University Council New policy drafted.